IMPROVED CFM MODE SYSTEM

FIELD OF THE INVENTION

The present invention relates to block cipher systems in general, and in particular to block cipher systems in CFM mode.

BACKGROUND OF THE INVENTION

Block ciphers are well known in the art, as is the use of block ciphers in Cipher Feedback mode (CFM), also known as Cipher Feed Back (CFB) mode. CFM mode was originally defined as a mode of operation of the well known DES system; see, for example, the following references:

1. NIST, FIPS Publication 81: DES Modes of Operation, 1980, which is available on the Internet at:

csrc.nist.gov/publications/fips/fips81/fips81.htm

2. ANSI, American National Standard X3.106-1983 (R1966): Data Encryption Algorithm, Modes of Operations for the, 1983.

A short description of CFM mode may be found on the Internet at:

www.rsasecurity.com/rsalabs/faq/2-1-4-4.html

The disclosures of all references mentioned above and throughout the present specification are hereby incorporated herein by reference.

SUMMARY OF THE INVENTION

The present invention seeks to provide an improved block cipher system, particularly but not exclusively useful for hardware-based encryption and decryption, especially for encryption and decryption of digital content.

In general, devices which encrypt and decrypt digital content must perform both encryption and decryption of data. Preferably, in order to simplify hardware design and minimize hardware gate count, the inventors of the present invention believe that the following requirements should preferably be met:

1. An encryption engine should preferably be provided in hardware for only one direction of a block cipher.

2. Data to be encrypted / decrypted (referred to herein as "data") comprises a plurality of packets. Encryption / decryption of a packet must in no way relate to any previous packet or packets. In other words, it is prohibited to have any "chaining" from one packet to another in decryption. The typical reason for the prohibition of "chaining" is that the physical stream to be decrypted is typically multiplexed from multiple logical stream, so any "chaining" information must be stored and managed for each logical stream independently; persons skilled in the art will appreciate that such a "heavy" requirement should be avoided .

3. The encryption / decryption key is changed much less often than packets arrive; therefore, many packets are encrypted with the same key.

4. Packet encryption and decryption should be performed in one pass.

5. Certain bits of the packet must not be affected by encryption and decryption. That is, certain bits must stay "in the clear"; bits, bytes, or data that

must stay in the clear are also termed herein "Must Stay Clear" or "MSC" bits, bytes or data. The reason for the requirement of certain bits being unaffected by encryption and decryption is in order to have some information about the stream available in the clear even before decryption. For example, and without limiting the generality of the foregoing, in an MPEG-2 transport stream the four first bytes of each packet stay in the clear; the four first bytes provide: information needed for demultiplexing; information as to whether the packet is encrypted at all; if the packet is encrypted, information as to whether the packet is encrypted with even or odd key; and other information as is well known in the art. In some packets, the header indicates that an initial part of the packet is the "adaptation field" which provides some other information necessary for the receiver; such information must always stay in the clear as well. Optionally a broadcaster may choose to send even part of video information in the clear, for example to make search easier in personal video recorder (PVR) systems.

Prior art encryption systems address the above-mentioned requirements only partially; in particular, requirement 1 is not addressed.

Reference is now made to Figs. 1A and 1B, which are simplified block diagram illustrations of a prior art block cipher system operating in CFM mode. Fig. 1A illustrates encryption, while Figs. 1B illustrates decryption. Persons skilled in the art will appreciate that, without requirement 4, it is possible to use any appropriate block cipher in CFM mode:

$$C_0 = IV$$

$$C_i = E_K(C_{i-1})\ XOR\ P_i$$

where $0 < i \leq$ the number of blocks being processed.

Where

$$P_i, C_i$$

are the i - th blocks of plaintext and ciphertext respectively, E is any appropriate block mode cipher, K is a key, and IV is an initial value, which may optionally comprise a publicly known initial value.

The corresponding decryption method is:

$$C_0 = IV$$

$$P_i = E_K(C_{i-1})\ XOR\ C_i$$

where $0 < i \leq$ the number of blocks being processed.

As is well known in the art, CFM mode is intended to allow a block cipher to be used as if it were a stream cipher, so that processing may occur on a byte-by-byte basis or even on a bit-by-bit basis, rather than on a block-by-block basis.

The present invention, in preferred embodiments thereof, provides improved block cipher systems which are intended to better address the above-mentioned requirements.

There is thus provided in accordance with a preferred embodiment of the present invention a method for producing at least one ciphertext block from at least one plaintext block using a block cipher E and a key K, the method including receiving n plaintext blocks, wherein n is an integer greater than 0, setting Q_0 equal to an initial value, and for each plaintext block of the n plaintext

blocks: computing $Q_i = E_K(Q_{i-1})\ XOR\ P_i$; and computing $C_i = M(P_i, Q_i)$, thereby producing n ciphertext blocks, wherein $0 < i <= n$, and P_i denotes an i - th plaintext block of the n plaintext blocks, and C_i denotes an i - th ciphertext block of the n ciphertext blocks, and *M* is a selector function which, for each bit C_{ij} of block C_i, selects a first argument of *M* if bit P_{ij} is not to be encrypted, and selects a second argument of *M* if bit P_{ij} is to be encrypted.

Further in accordance with a preferred embodiment of the present invention *M* is chosen in accordance with a standard indicating bits that are not to be encrypted.

Still further in accordance with a preferred embodiment of the present invention the standard includes one of the following an audio standard, a video standard, and an audio-video standard.

Additionally in accordance with a preferred embodiment of the present invention the standard includes MPEG-2.

There is also provided in accordance with another preferred embodiment of the present invention a method for producing at least one ciphertext block from at least one plaintext block using a block cipher *E* and a key *K*, the method including receiving n plaintext blocks, wherein n is an integer greater than 0, and an initial value *IV*, computing $IV' = M(P_1, IV)$, computing $Q_0 = H(IV')$, and for each plaintext block of the n plaintext

blocks: computing $Q_i = E_K(Q_{i-1})\ XOR\ P_i$; and computing $C_i = M(P_i, Q_i)$, thereby producing n ciphertext blocks, wherein $0 < i <= n$, and H is a hash function, and P_i denotes an i - th plaintext block of the n plaintext blocks, and C_i denotes an i - th ciphertext block of the n ciphertext blocks, and M is a selector function which, for each bit C_{ij} of block C_i, selects a first argument of M if bit P_{ij} is not to be encrypted, and selects a second argument of M if bit P_{ij} is to be encrypted.

Further in accordance with a preferred embodiment of the present invention H includes SHA1.

Still further in accordance with a preferred embodiment of the present invention $H(IV')$ includes $E_K(IV')\ XOR\ IV'$.

Additionally in accordance with a preferred embodiment of the present invention M is chosen in accordance with a standard indicating bits that are not to be encrypted.

Moreover in accordance with a preferred embodiment of the present invention the standard includes one of the following an audio standard, a video standard, and an audio-video standard.

Further in accordance with a preferred embodiment of the present invention the standard includes MPEG-2.

There is also provided in accordance with another preferred embodiment of the present invention, in a method for producing at least one ciphertext block from at least one plaintext block using a block cipher E and a key K in a stream mode, wherein P_i denotes an i - th plaintext block, and C_i denotes an i - th ciphertext block, an improvement including for each bit C_{ij} of block C_i, selecting P_{ij} as an output if bit P_{ij} is not to be encrypted.

Further in accordance with a preferred embodiment of the present invention the stream mode includes CFM mode.

There is also provided in accordance with another preferred embodiment of the present invention apparatus for producing at least one ciphertext block from at least one plaintext block using a block cipher E and a key K, the at least one plaintext block including n plaintext blocks, the at least one ciphertext block including n ciphertext blocks, wherein n is an integer greater than 0, the apparatus including an initialization unit for setting Q_0 equal to an initial value, and a computation unit operative, for each plaintext block of the n plaintext blocks: to compute $Q_i = E_K(Q_{i-1})\ XOR\ P_i$; and to compute $C_i = M(P_i, Q_i)$, wherein 0 < i <= n, and P_i denotes an i - th plaintext block of the n plaintext blocks, and C_i denotes an i - th ciphertext block of the n ciphertext blocks, and M is a selector function which, for each bit C_{ij} of block C_i, selects a

first argument of M if bit P_{ij} is not to be encrypted, and selects a second argument of M if bit P_{ij} is to be encrypted.

There is also provided in accordance with yet another preferred embodiment of the present invention apparatus for producing at least one ciphertext block from at least one plaintext block using a block cipher E, a key K, and an initial value IV, the at least one plaintext block including n plaintext blocks, the at least one ciphertext block including n ciphertext blocks, wherein n is an integer greater than 0, the apparatus including a first computation unit for computing $IV' = M(P_1, IV)$, a second computation unit for computing $Q_0 = H(IV')$, and a third computation unit operative, for each plaintext block of the n plaintext blocks: to compute $Q_i = E_K(Q_{i-1})\ XOR\ P_i$, and to compute $C_i = M(P_i, Q_i)$, wherein $0 < i <= n$, and H is a hash function, and P_i denotes an i - th plaintext block of the n plaintext blocks, and C_i denotes an i - th ciphertext block of the n ciphertext blocks, and M is a selector function which, for each bit C_{ij} of block C_i, selects a first argument of M if bit P_{ij} is not to be encrypted, and selects a second argument of M if bit P_{ij} is to be encrypted.

There is also provided in accordance with still another preferred embodiment of the present invention, in apparatus for producing at least one ciphertext block from at least one plaintext block using a block cipher E and a key K in a stream mode, wherein P_i denotes an i - th plaintext block, and C_i denotes an i - th ciphertext block, an improvement including a selector unit operative, for each bit C_{ij} of block C_i, to select P_{ij} as an output if bit P_{ij} is not to be encrypted.

There is also provided in accordance with yet another preferred embodiment of the present invention a method for producing at least one plaintext block from at least one ciphertext block encrypted using a block cipher E and a key K, the method including receiving n ciphertext blocks, where n is an integer greater than 0, setting Q_0 equal to an initial value, and for each ciphertext block of the n ciphertext blocks: computing $Q'_i = E_K(Q_{i-1})\ XOR\ C_i$; computing $P_i = M(C_i\ ,\ Q'_i)$; and computing $Q_i = M(Q'_i\ ,\ C_i)$, thereby producing n plaintext blocks, wherein 0 < i <= n, and P_i denotes an i - th plaintext block of the n plaintext blocks, and C_i denotes an i - th ciphertext block of the n ciphertext blocks, and M is a selector function which, for each bit C_{ij} of block C_i, selects a first argument of M if bit P_{ij} is not encrypted, and selects a second argument of M if bit P_{ij} is encrypted.

Further in accordance with a preferred embodiment of the present invention M is chosen in accordance with a standard indicating bits that are not encrypted.

Still further in accordance with a preferred embodiment of the present invention the standard includes one of the following an audio standard, a video standard, and an audio-video standard.

Additionally in accordance with a preferred embodiment of the present invention the standard includes MPEG-2.

There is also provided in accordance with another preferred embodiment of the present invention a method for producing at least one plaintext block from at least one ciphertext block using a block cipher E and a key K, the method including receiving n ciphertext blocks, wherein n is an integer greater than 0, and an initial value IV, computing $IV' = M(P_1, IV)$, computing $Q_0 = H(IV')$, and for each ciphertext block of the n ciphertext blocks: computing $Q'_i = E_K(Q_{i-1})\ XOR\ C_i$, computing $P_i = M(C_i, Q'_i)$, and computing $Q_i = M(Q'_i, C_i)$, thereby producing n plaintext blocks, wherein 0 < i <= n, and H is a hash function, and P_i denotes an i - th plaintext block of the n plaintext blocks, and C_i denotes an i - th ciphertext block of the n ciphertext blocks, and M is a selector function which, for each bit C_{ij} of

block C_i, selects a first argument of M if bit P_{ij} is not encrypted, and selects a second argument of M if bit P_{ij} is encrypted.

Further in accordance with a preferred embodiment of the present invention H includes SHA1.

Still further in accordance with a preferred embodiment of the present invention $H(IV')$ includes $E_K(IV')\ XOR\ IV'$.

Additionally in accordance with a preferred embodiment of the present invention M is chosen in accordance with a standard indicating bits that are not encrypted.

Moreover in accordance with a preferred embodiment of the present invention the standard includes one of the following an audio standard, a video standard, and an audio-video standard.

Further in accordance with a preferred embodiment of the present invention the standard includes MPEG-2.

There is also provided in accordance with another preferred embodiment of the present invention, in a method for producing at least one plaintext block from at least one ciphertext block using a block cipher E and a key K in a stream mode, wherein P_i denotes an i - th plaintext block of the plurality of plaintext blocks, and C_i denotes an i - th ciphertext block of the plurality of

ciphertext blocks, an improvement including for each bit P_{ij} of block P_i, selecting C_{ij} as an output if bit C_{ij} is not encrypted.

Further in accordance with a preferred embodiment of the present invention the stream mode includes CFM mode.

There is also provided in accordance with another preferred embodiment of the present invention apparatus for producing at least one plaintext block from at least one ciphertext block encrypted using a block cipher E and a key K, the at least one ciphertext block including n ciphertext blocks, the at least one plaintext block including n plaintext blocks, wherein n is an integer greater than 0, the apparatus including initialization apparatus for setting Q_0 equal to an initial value, and a computation unit operative, for each ciphertext block of the n ciphertext blocks: to compute $Q'_i = E_K(Q_{i-1})\ XOR\ C_i$; to compute $P_i = M(C_i, Q'_i)$; and to compute $Q_i = M(Q'_i, C_i)$, wherein $0 < i <= n$, and P_i denotes an i - th plaintext block of the n plaintext blocks, and C_i denotes an i - th ciphertext block of the n ciphertext blocks, and M is a selector function which, for each bit C_{ij} of block C_i, selects a first argument of M if bit P_{ij} is not encrypted, and selects a second argument of M if bit P_{ij} is encrypted.

There is also provided in accordance with yet another preferred embodiment of the present invention apparatus for producing at least one plaintext

block from at least one ciphertext block using a block cipher E and a key K, the at least one ciphertext block including n ciphertext blocks, the at least one plaintext block including n plaintext blocks, wherein n is an integer greater than 0, the apparatus including a first computation unit for computing $IV' = M(P_1, IV)$, a second computation unit for computing $Q_0 = H(IV')$, and a third computation unit operative, for each ciphertext block of the n ciphertext blocks: to compute $Q'_i = E_K(Q_{i-1})\ XOR\ C_i$; to compute $P_i = M(C_i, Q'_i)$; and to compute $Q_i = M(Q'_i, C_i)$, wherein 0 < i <= n, and H is a hash function, and P_i denotes an i - th plaintext block of the n plaintext blocks, and C_i denotes an i - th ciphertext block of the n ciphertext blocks, and M is a selector function which, for each bit C_{ij} of block C_i, selects a first argument of M if bit P_{ij} is not encrypted, and selects a second argument of M if bit P_{ij} is encrypted.

There is also provided in accordance with still another preferred embodiment of the present invention, in apparatus for producing at least one plaintext block from at least one ciphertext block using a block cipher E and a key K in a stream mode, wherein P_i denotes an i - th plaintext block of the plurality of plaintext blocks, and C_i denotes an i - th ciphertext block of the plurality of

ciphertext blocks, an improvement including a selector unit operative, for each bit P_{ij} of block P_i, to select C_{ij} as an output if bit C_{ij} is not encrypted.

BRIEF DESCRIPTION OF THE DRAWINGS

The present invention will be understood and appreciated more fully from the following detailed description, taken in conjunction with the drawings in which:

Figs. 1A and 1B are simplified block diagram illustrations of a prior art block cipher system operating in CFM mode;

Figs. 2A and 2B are simplified block diagram illustrations of a block cipher system constructed and operative in accordance with a first preferred embodiment of the present invention; and

Figs. 3A and 3B are simplified block diagram illustrations of a block cipher system constructed and operative in accordance with a second preferred embodiment of the present invention.

DETAILED DESCRIPTION OF PREFERRED EMBODIMENTS

In accordance with a first preferred embodiment of the present invention, a block cipher system based generally on CFM is provided, with a modification made to meet requirement 4 mentioned above. The modification is preferably as follows:

$$Q_0 = IV$$

$$Q_i = E_K(Q_{i-1})\ XOR\ P_i$$

$$C_i = M(P_i, Q_i)$$

where $0 < i \leq$ the number of blocks being processed.

where for each bit

$$C_{ij}$$

of block

$$C_i$$

function M selects between its first argument (in this case P_{ij}) and its second argument (in this case Q_{ij}) depending on whether the present bit of the plaintext should be encrypted or not. For a bit C_{ij}, the result of function M (termed herein a "selector function", and also known in the art as a multiplexer) may depend on all preceding blocks of the plaintext, and on those preceding bits of the plaintext in the current block C_i that are not encrypted.

It is appreciated that the function M is chosen based on operational requirements which specify which bits should or should not be encrypted, as is explained in more detail below with reference to Figs. 2A, 2B, 3A, and 3B.

The corresponding decryption method is:

$$Q_0 = IV$$

$$Q'_i = E_K(Q_{i-1})\ XOR\ C_i$$

$$P_i = M(C_i\ ,\ Q'_i)$$

$$Q_i = M(Q'_i\ ,\ C_i)$$

where $0 < i \leq$ the number of blocks being processed.

Persons skilled in the art will appreciate that the first preferred embodiment has a weakness, compared with regular use of the block cipher, as follows. For all packets encrypted with the same key K the first block

$$P_1$$

will be encrypted by XOR with the same pad

$$E_K(IV)$$

which method is insecure. More generally, in a case where there are several packets whose first n blocks are identical and $(n+1)$-th blocks differ, the XOR pads of those packets will be identical up to the $(n+1)$-th block, and different from the $(n+2)$-th block on.

Nevertheless, in contexts where making it easier for an unauthorized person to decrypt a small part of the content is not critical, and there is much

variability between packets, as in video- and audio- streams, the indicated weakness may be tolerable.

Without limiting the generality of the foregoing, the special case of MPEG Transport Stream, such as in MPEG-2 (as described in ISO / IEC 13818-1, Information technology - Generic coding of moving pictures and associated audio information: Systems), will now be considered. Persons skilled in the art will appreciate that MPEG-2 is provided as an example only, and is not meant to be limiting.

Reference is now made to Figs. 2A and 2B, which are simplified block diagram illustrations of a block cipher system constructed and operative in accordance with the first preferred embodiment of the present invention. Figs. 2A and 2B illustrate the special case of the first preferred embodiment of the present invention, used in an MPEG-2 system. Fig. 2A illustrates encryption, while Fig. 2B illustrates decryption. Figs. 2A and 2B are self-explanatory with reference to the discussion above and below.

In MPEG-2 each transport packet comprises 188 bytes. The first 4 first bytes (bytes 0 - 3) comprise the packet header. The first 4 bytes are always MSC bytes that must stay in the clear; that is, the first 4 bytes must not be encrypted. As is well known in the art of MPEG-2, depending on one of the bits in those bytes, there may be an additional adaptation field immediately after the header that also must stay in the clear (MSC); in such a case, byte 4 contains the length of the adaptation field. The rest of the packet should be encrypted / decrypted.

If, for example, the well-known prior art AES (which is described in FIPS Publication 197, November 26, 2001, Announcing the Advanced Encryption Standard (AES, available on the Internet at csrc.nist.gov/publications/fips/fips197/fips-197.pdf) is used as a block cipher (with 16-byte blocks), each packet may be padded with a 4-byte IV (which may optionally be publicly known) before the 4 first bytes; this 4-byte IV is in addition to the 16-byte IV

$$C_0$$

After encryption, the 4 first bytes of

$$C_1$$

will be discarded; therefore, it does not matter whether the first 4 bytes should be encrypted.

In accordance with a second preferred embodiment of the present invention, which is believed by the inventor to be stronger against attack than the first preferred embodiment of the present invention, the clear part of

$$P_1$$

is mixed into the initial value. For example and without limiting the generality of the foregoing, the following method may be used:

$$IV' = M(P_1, IV)$$

$$Q_0 = E_K(IV')\ XOR\ IV'$$

$$Q_i = E_K(Q_{i-1})\ XOR\ P_i$$

$$C_i = M(P_i, Q_i)$$

where $0 < i \leq$ the number of blocks being processed.

It is appreciated that the present invention is not limited to the use of the formula

$$Q_0 = E_K(IV') \; XOR \; IV'$$

Rather, any appropriate hash function of IV' may be used. In general, for an appropriate hash function H:

$$Q_0 = H(IV')$$

For example, and without limiting the generality of the foregoing, the well-known SHA1 hash function may be used. The SHA1 hash function is described, for example, in the following two publications:

FIPS PUB 180-1, published 17 April 1995 and entitled "Secure Hash Standard", available on the Internet at: www.itl.nist.gov/fipspubs/fip180-1.htm ; and

RFC 3174, published September 2001 and entitled "US Secure Hash Algorithm 1 (SHA1), available on the Internet at www.ietf.org/rfc/rfc3174.txt?number=3174

The corresponding decryption method is:

$$IV' = M(P_1, IV)$$

$$Q_0 = H(IV')$$

$$Q'_i = E_K(Q_{i-1})\ XOR\ C_i$$

$$P_i = M(C_i\,,\ Q'_i)$$

$$Q_i = M(Q'_i\,,\ C_i)$$

where $0 < i \leq$ the number of blocks being processed.

Persons skilled in the art will appreciate that, in the second preferred embodiment of the present invention, any two packets that have a different initial clear part of the first block will have a completely different XOR pad. Therefore, the number of packets with the same XOR pad, even for the first block only, will decrease, making it more difficult to use the weakness described above with reference to the first preferred embodiment of the present invention.

Without limiting the generality of the foregoing, the special case of MPEG-2, as described above, will now be considered in connection with the second preferred embodiment of the present invention. Persons skilled in the art will appreciate that MPEG-2 is provided as an example only, and is not meant to be limiting.

Reference is now made to Figs. 3A and 3B, which are simplified block diagram illustrations of a block cipher system constructed and operative in accordance with the second preferred embodiment of the present invention. Figs. 3A and 3B illustrate the special case of the first preferred embodiment of the present invention, used in an MPEG-2 system. Fig. 3A illustrates encryption, while Fig. 3B illustrates decryption. Figs. 3A and 3B are self-explanatory with reference to the discussion above and below.

It is appreciated that, in Figs. 3A and 3B, the particular example of an XOR function as the function F is depicted; as described above, the present invention is not limited to use of the XOR function.

The above discussion of the special case of MPEG-2 with reference to Figs. 2A and 2B also applies to Figs. 3A and 3B.

It is appreciated that various features of the invention which are, for clarity, described in the contexts of separate embodiments may also be provided in combination in a single embodiment. Conversely, various features of the invention which are, for brevity, described in the context of a single embodiment may also be provided separately or in any suitable subcombination.

It will be appreciated by persons skilled in the art that the present invention is not limited by what has been particularly shown and described hereinabove. Rather the scope of the invention is defined only by the claims which follow: